REMARKS

Claims 1-7, 9-14, 16-20, and 22 were pending in the application and all were rejected. Claims 1, 4, 7, 9, 12 have been amended. Applicant respectfully requests reconsideration.

CLAIM REJECTIONS UNDER 35 USC §103

The Office Action finally rejected claims 1-3, 9-12, and 22 under 35 USC 103(a), as being unpatentable over Schweitzer et al. (US Patent No. 5,850, 450) in view of Hopkins, as before, and further in view of Kocher et al. (USP 6304658).

The Office Action at page 5 concedes that "The combination of Schweitzer and Hopkins does not teach: If the public cryptographic key has been revoked abort signing of the message," but alleges that "However, these features are well known in the art and would have been an obvious modification of the system disclosed by the combination of Schweitzer and Hopkins as introduced by Kocher." Applicant respectfully traverses this finding, which appears to be based on this sentence from Kocher's Abstract: "In addition to producing useful cryptographic results, a typical leak-resistant cryptographic operation modifies or updates secret key material in a manner designed to render useless any information about the secrets that may have previously leaked from the system."

It is apparent from Kocher's Abstract that Kocher does not teach the claimed element of aborting signing of the message if the *public* key has been revoked. Kocher provides for the ability to invalidate secret key material associated with a system leak, but Kocher does not abort signing of a message when the public key is revoked; therefore the Examiner imports into the

claim an exemplary limitation drawn from paragraph [0064] of Applicant's disclosure: "[0064] The generation of the signature value i, y, a is addressed hereafter with regard to some more mathematical aspects. It is assumed that the message m is to be signed. If the public cryptographic key pk has been revoked, e.g., because the secret cryptographic key sk has been leaked, or if i > I, i.e., the maximal number of producable signature values has been reached, then signing is aborted." "Generally, particular limitations or embodiments appearing in the specification will not be read into the claims." *Loctite Corp. v. Ultraseal Ltd.*, 781 F.2d 861, 867, 228 USPQ 90, 93 (Fed. Cir. 1985).

The signature scheme as recited in claim 1 is patentable over the cited references because none of the cited references provide for the limitation of aborting the message signing if the public cryptographic key has been revoked. Further, claim 1 has been amended to recite an additional limitation of "publishing a parameter as part of the public cryptographic key, wherein said parameter controls a time-period during which a user can take to note that the secret cryptographic key was compromised." None of the cited references teach or suggest this limitation. Support for this limitation can be found in paragraphs [0077] and [0090] of Applicant's specification as published in United States Patent Publication Number 2006/0233364.

Independent claims 1 and 12 are patentable over the cited references for at least the reasons as discussed above. Claims 2-3, 9-11, and 22 are also patentable by virtue of their dependence on the patentable claims.

The Office Action rejected claims 4-7, 13, 14, and 16-20 under 35 USC 103(a) as being unpatentable over Hopkins in view of Kocher.

Claims 4-7, 13, 14, and 16-20 are patentable over the cited references because they depend on claims that contain limitations not taught or suggested by the cited references.

CONCLUSION

For the foregoing reasons, Applicant respectfully requests allowance of the pending claims. The Director is hereby authorized to charge any fees which may be required, including any petition for extension of time fees under §1.17, or credit any overpayment, to Deposit Account Number 50--0510.

Respectfully submitted,

/Michael J. Buchenhorner/

Michael J. Buchenhorner
Reg. No. 33,162

Date: September 8, 2009

Michael Buchenhorner, P.A.
8540 S.W. 83 Street
Miami, Florida 33143
(305) 273-8007 (voice)
(305) 595-9579 (fax)